IN THE CLAIMS:

Claims 1, 3-6, 11, 14, 15, 17-20, 25, 27, 29, 31, 32, and 35 are amended herein. All pending claims and their present status are produced below.

1   1.   (Currently Amended) A method of tracking a security state for an intermodal
2   container through a global supply chain, comprising:
3   receiving ~~credentials~~ a credential from a first trusted agent confirming the first trusted
4   agent has trusted status;
5   receiving a required body of information concerning an intermodal container from the
6   first trusted agent located at a first checkpoint;
7   initiating a security state for the intermodal container with the required body of
8   information ~~submitted by the first trusted agent located at a first checkpoint~~;
9   ~~continuously~~ monitoring the security state of the container during transport between
10   the first checkpoint and a second checkpoint, the security state adapted to
11   change responsive a security breach;
12   receiving ~~credentials~~ a credential from a second trusted agent confirming the second
13   trusted agent has trusted status; and
14   sending the security state to the second trusted agent located at the second checkpoint
15   for validation.

1   2.   (Original) The method of claim 1, wherein the step of initiating the security
2   state comprises initiating the security state to a secure state responsive to an inspection by the
3   first trusted agent.

1   3.   (Currently Amended) The method of claim 1, wherein the step of
2   ~~continuously~~ monitoring the security state comprises changing the security state responsive
3   to a security breach defined by security business rules.

1   4.   (Currently Amended) The method of claim 1, wherein ~~the step of initiating~~
2   ~~the security state comprises initiating the security state with a~~ the required body of
3   information ~~comprising~~ comprises an expected transport route between the first checkpoint
4   and the second checkpoint, and wherein the step of monitoring the security state comprises

5   changing the security state if the actual transport route deviates from the expected transport

6   route.

1   5.   (Currently Amended) The method of claim 1, wherein ~~the step of initiating~~

2 ~~the security state comprises initiating the security state with a~~ the required body of

3   information ~~comprising~~ comprises information related to authorized unsealing of the

4   container, and wherein the step of monitoring the security state comprises changing the

5   security state if the container is unsealed without authorization between the first checkpoint

6   and the second checkpoint.

1   6.   (Currently Amended) The method of claim 1, wherein ~~the step of initiating~~

2 ~~the security state comprises initiating the security state with~~ the required body of information

3 ~~comprising~~ comprises information concerning a unique identifier assigned to a seal that locks

4   the container, and wherein the step of monitoring the security state comprises using the

5   unique identifier to continually monitor the seal for a status.

1   7.   (Original) The method of claim 6, wherein the status comprises one from the

2   group consisting of: door open, attempt to open door, door closed, door locked, right door

3   open, and more than one door open.

1   8.   (Original) The method of claim 6, wherein the status comprises an

2   environmental state from the group consisting of: temperature, humidity, vibration, shock,

3   light, and radiation.

1   9.   (Original) The method of claim 1, further comprising the steps of:

2   detecting the security breach; and

3   resetting the security state responsive to the second agent submitting an indication

4   that the container was resecured.

1   10.   (Original) The method of claim 1, further comprising the steps of:

2   receiving an inspection request from an authority; and

3   changing the security state responsive to the inspection request.

1   11.   (Currently Amended) The method of claim [[1]] 10, further comprising the

2 steps step of:

3   submitting [[a]] the required body of information, including the information, to [[an]]

4   the authority;

5   wherein the authority sends the inspection request responsive to the required body of

6   information.

1   12.   (Original) The method of claim 1, wherein the first agent is located at an

2 origin port of an export country and the second agent is located at a destination port of an

3 import country.

1   13.   (Original) The method of claim 1, wherein the step of monitoring comprises

2 the steps of:

3   receiving monitor information from a first reader at the first checkpoint through a first

4   control center;

5   receiving monitor information from a second reader on a transportation device; and

6   receiving monitor information from a third reader at the second checkpoint through a

7   second control center.

1   14.   (Currently Amended) The method of claim [[1]] 13, wherein the container

2 comprises an RFID (Radio Frequency IDentification) tag, and the first, second, and third

3 readers each comprise an RFID reader.

1   15.   (Currently Amended) A security state system for tracking a container through

2 a global supply chain, comprising:

3   a first receiving module for receiving credentials a credential from a first trusted

4   agent confirming the first trusted agent has trusted status;

5   a second receiving module for receiving a required body of information concerning a

6   container submitted by the first trusted agent located at a first checkpoint, the

7   second receiving module coupled to the first receiving module;

8   a required body of information module to store the required body of information-

9   ~~concerning the container~~ submitted by [[a]] <u>the</u> first trusted agent ~~located at a~~

10   ~~first checkpoint~~, the required body of information module coupled to the

11   <u>second</u> receiving module;

12   a <u>~~second~~ third</u> receiving module for receiving ~~credentials~~ <u>a credential</u> from a second

13   trusted agent confirming the second trusted agent has trusted status; and

14   a security state module, coupled to the <u>required body of</u> information module and the

15   <u>~~second~~ third</u> receiving module, the security state module initiating the security

16   state based on the <u>required body of</u> information, ~~continuously~~ <u>the security</u>

17   <u>state module</u> monitoring the security state between the first checkpoint and a

18   second checkpoint, the security state adapted to change responsive to a

19   security breach, and the security state module sending the security state to a

20   second trusted agent at the second checkpoint for validation.

1   16.   (Original) The system of claim 15, wherein the security state module initiates

2   the security state to a secure state responsive to an inspection by the first trusted agent.

1   17.   (Currently Amended) The system of claim 15, wherein the security state

2   module ~~further comprises to~~ change<u>s</u> the security state responsive to a security breach

3   defined by security business rules.

1   18.   (Currently Amended) The system of claim 15, wherein the <u>required body of</u>

2   information comprises an expected transport route between the first checkpoint and the

3   second checkpoint, and wherein the security state module changes the security state if the

4   actual transport route deviates from the expected transport route.

1   19.   (Currently Amended) The system of claim 15, wherein the <u>the required body</u>

2   <u>of</u> information comprises authorized unsealing of the container, and wherein the security

3   state module changes the security state if the container is unsealed without authorization

4   between the first checkpoint and the second checkpoint.

1   20.   (Currently Amended) The system of claim 15, wherein the <u>required body of</u>

2   information comprises a unique identifier assigned to a seal that locks the container, and

3   wherein the security state module uses the unique identifier to continually monitor the seal

4   for a status.

1   21.   (Original) The system of claim 20, wherein the status comprises one from the

2   group consisting of: door open, attempt to open door, door closed, door locked, right door

3   open, and more than one door open.

1   22.   (Original) The system of claim 20, wherein the status comprises an

2   environmental state from the group consisting of: temperature, humidity, vibration, shock,

3   light, and radiation.

1   23.   (Original) The system of claim 15, further comprising a seal device to detect

2   a security breach, wherein the security state module resets the security state responsive to the

3   second agent submitting an indication that the container was resecured.

1   24.   (Original) The system of claim 15, wherein the security state module changes

2   the security state responsive to receiving an inspection request from a customs control center.

1   25.   (Currently Amended) The system of claim 15, wherein the security state

2   module submits [[a]] the required body of information, including the information, to a

3   customs control center [[,]] and receives an inspection request responsive to the required

4   body of information.

1   26.   (Original) The system of claim 15, wherein the first agent is located at an

2   origin port of an export country and the second agent is located at a destination port of an

3   import country.

1   27.   (Currently Amended) The system of claim 15, wherein the required body of

2   information module receives the required body of information from a first reader at the first

3   checkpoint through a first control center, the security state module receives continuous

4   monitoring information from a second reader; and receives a validation confirmation from a

5   third reader at the second checkpoint through a second control center.

1   28.   (Previously presented) The system of claim 27, wherein the container
2   comprises an RFID (radio frequency identification) tag, and the first, second, and third
3   readers comprise an RFID reader.

1   29.   (Currently Amended) A computer product having a computer-readable
2   medium having computer program instructions embodied thereon capable of causing a
3   computer to perform a method of tracking a security state for an intermodal container
4   through a global supply chain, the method comprising:
5   receiving ~~credentials~~ a credential from a first trusted agent confirming the first trusted
6   agent has trusted status;
7   receiving a required body of information concerning an intermodal container from the
8   first trusted agent located at a first checkpoint;
9   initiating a security state for the intermodal container with the required body of
10   information ~~submitted by the first trusted agent located at a first checkpoint~~;
11   ~~continuously~~ monitoring the security state of the container during transport between
12   the first checkpoint and a second checkpoint, the security state adapted to
13   change responsive a security breach;
14   receiving ~~credentials~~ a credential from a second trusted agent confirming the second
15   trusted agent has trusted status; and
16   sending the security state to the second trusted agent located at the second checkpoint
17   for validation.

1   30.   (Original) The computer product of claim 29, wherein the step of initiating
2   the security state comprises initiating the security state to a secure state responsive to an
3   inspection by the first trusted agent.

1   31.   (Currently Amended) The computer product of claim 29, wherein the step of
2   ~~continuously~~ monitoring the security state comprises changing the security state responsive
3   to a security breach defined by security business rules.

1   32.   (Currently Amended) The computer product of claim 29, wherein the ~~step of~~

2   ~~initiating the security state comprises initiating the security state with a~~ required body of

3   information ~~comprising~~ <u>comprises</u> information concerning a unique identifier assigned to a

4   seal that locks the container, and wherein the step of monitoring the security state comprises

5   using the unique identifier to continually monitor the seal for a status.

1   33.   (Original) The computer product of claim 29, further comprising the steps of:

2   detecting the security breach; and

3   resetting the security state responsive to the second agent submitting an indication

4   that the container was resecured.

1   34.   (Original) The computer product of claim 29, further comprising the steps of:

2   receiving an inspection request from an authority; and

3   changing the security state responsive to the inspection request.

1   35.   (Currently Amended) The computer product of claim [[29]] <u>34</u>, further

2   comprising the ~~steps~~ <u>step</u> of:

3   submitting [[a]] <u>the</u> required body of information~~, including the information,~~ to [[an]]

4   <u>the</u> authority;

5   wherein the authority sends the inspection request responsive to the required body of

6   information.

7

1   36.   (Original) The computer product of claim 29, wherein the first agent is

2   located at an origin port of an export country and the second agent is located at a destination

3   port of an import country.